IN THE UNITED STATES PATENT AND TRADEMARK OFFICE
BEFORE THE BOARD OF PATENT APPEALS AND INTERFERENCES

ATTY. DOCKET NO.: FR919990055US1

IN RE APPLICATION OF:	§	
	§	
ALINE FICHOU ET AL.	§	EXAMINER: **DOUGLAS B. BLAIR**
	§	
SERIAL NO.: **09/811,038**	§	CONFIRMATION NO.: **5687**
	§	
FILED: **MARCH 16, 2001**	§	ART UNIT: **2142**
	§	
FOR: **SYSTEM AND METHOD FOR RESERVING A VIRTUAL CONNECTION IN AN IP NETWORK**	§	

APPEAL BRIEF UNDER 37 C.F.R. 1.192

Mail Stop Appeal Briefs - Patents
Commissioner for Patents
P.O. Box 1450
Alexandria, Virginia 22313-1450

Sir:

This Appeal Brief is submitted in support of an Appeal of the final rejection of claims 8-23. A Notice of Appeal in this case was filed and received by the Patent Office on June 5, 2006. Applicants previously filed a Request for Extension for Response Within the First Month; therefore, no additional extension-of-time fee is believed to be due. Please charge the fee of $500.00 due under 37 C.F.R. § 1.17(c) and any additional prosecution fees, if required, to **IBM Corporation's Deposit Account No. 09-0457**.

REAL PARTY IN INTEREST

The real party in interest in the present Application is International Business Machines Corporation, the Assignee of the present application as evidenced by the Assignment set forth at reel 011795, frame 0107 et. seq. of the USPTO assignment records.

RELATED APPEALS AND INTERFERENCES

There are no other appeals or interferences known to Appellants, the Appellants' legal representative, or assignee, which directly affect or would be directly affected by or have a bearing on the Board's decision in the pending appeal.

STATUS OF CLAIMS

Claims 8-23 stand finally rejected as noted in the final Office Action dated February 16, 2006. The rejection of claims 8-23 is appealed.

STATUS OF AMENDMENTS

Appellant's Amendment A filed on September 8, 2004 was entered by the Examiner. No amendment to the claims was proposed or entered subsequent to Appellant's Amendment A dated September 8, 2004.

SUMMARY OF THE CLAIMED SUBJECT MATTER

Appellants' claimed invention covers a method/apparatus for reserving a virtual connection between source and destination workstations in which packets are transmitted between an ingress node communicating with the source workstation and an egress node communicating with the destination workstation. A key feature of the claimed invention is a two-part, sequentially significant verification relating to whether a virtual connection reservation request will be granted or denied. Namely, a reservation server first uses user information (user permissions, etc.) to validate the virtual connection reservation request. Next, and in response to user information validation of the request, the request is validated in terms of available network capacity.

Specifically, Appellants' **claim 8** recites a method for reserving a virtual connection from a source workstation to a destination workstation within a network to allow data packets to be transmitted between an ingress node of said source workstation and an egress node of said destination workstation (*see specification*, page 4, lines 1-10; **FIG. 1**, depicting IP network **14** connecting source workstation **10** with destination workstation **32** via ingress node **20** and egress node **24**; page 7, line 1 through page 8, line 14), said method comprising:

sending a reservation request for a virtual connection from said source workstation to a reservation server, (*see,* page 8, lines 16-26, describing with reference to **FIG. 2** constructing and sending a virtual connection reservation request from source workstation **10** to a reservation server) wherein said reservation server includes connection setup means for setting up a virtual connection that meets a predefined Quality of Service (QoS) requirement from said ingress node to said egress node (*see,* page 4, lines 10-16, describing the reservation server as including a user database and network database for storing information describing the network capacity required to set up a virtual connection; page 9, line 8 through page 11, line 9, describing with reference to **FIG. 3** a reservation server using a user database **50** and network database **56** to set up various virtual connection logistics including user authorization, and in which the connection would meet QoS specifications in terms of network bandwidth and capacity);

determining whether or not said reservation request can be validated based on user information within said source workstation, wherein said user information is accessible by said reservation server (*see,* page 4, lines 10-13, describing the reservation server as including a user database for storing authorized user identifications for accessing the reservation server and further storing the rights of the users; page 4, lines 16-19, describing verifying whether or not the reservation request can be validated in view of user information within the source workstation; page 9, lines 12-20, describing with reference to **FIG. 3** the reservation server initiating user authentication (step **48**) involving use of a database **50** storing user identification and profile information);

in response to a determination that said reservation request can be validated based on user information within said source workstation, determining whether or not the capacity of said network is sufficient to meet requirements of said reservation request (*see,* page 4, lines 19-22, describing a second verification performed, in addition to the user verification, to determine whether network

capacity is sufficient to meet the reservation request requirements; page 9, line 32 through page 10, line 7, explaining with reference to **FIG. 3**, that the if the user verification performed at step **52** fails, the reservation request is rejected and if the user verification is successful, the process continues with an assessment of network capacity (step **54**); and

in response to a determination that the capacity of said network being sufficient to meet requirements of said reservation request, establishing a virtual connection from said ingress node to said egress node (*see,* page 4, lines 22-26, describing virtual connection establishment performed in response to the network capacity verification; page 10, line 5 through page 11, line 2, describing with reference to **FIG. 3** that if at step **58** it is determined that network capacity is sufficient to accommodate the reservation request, virtual connection establishment continues with setting a flow identification (step **64**), updating a network database **56** (step **66**), and sending a reservation request acceptance (step **62**)).

Appellants' **claim 16** recites an apparatus for reserving a virtual connection from a source workstation to a destination workstation within a network to allow data packets to be transmitted between an ingress node of said source workstation and an egress node of said destination workstation (*see specification*, page 4, lines 1-10; **FIG. 1**, depicting IP network **14** connecting source workstation **10** with destination workstation **32** via ingress node **20** and egress node **24**; page 7, line 1 through page 8, line 14), said apparatus comprising:

means for sending a reservation request for a virtual connection from said source workstation to a reservation server, (*see,* page 8, lines 16-26, describing with reference to **FIG. 2** constructing and sending a virtual connection reservation request from source workstation **10** to a reservation server) wherein said reservation server includes connection setup means for setting up a virtual connection that meets a predefined Quality of Service (QoS) requirement from said ingress node to said egress node (*see,* page 4, lines 10-16, describing the reservation server as including a user database and network database for storing information describing the network capacity required to set up a virtual connection; page 9, line 8 through page 11, line 9, describing with reference to **FIG. 3** a reservation server using a user database **50** and network database **56** to set up various virtual connection logistics including user authorization, and in which the connection would meet QoS specifications in terms of network bandwidth and capacity);

means for determining whether or not said reservation request can be validated based on user information within said source workstation, wherein said user information is accessible by said reservation server (*see,* page 4, lines 10-13, describing the reservation server as including a user database for storing authorized user identifications for accessing the reservation server and further storing the rights of the users; page 4, lines 16-19, describing verifying whether or not the reservation request can be validated in view of user information within the source workstation; page 9, lines 12-20, describing with reference to **FIG. 3** the reservation server initiating user authentication (step **48**) involving use of a database **50** storing user identification and profile information);

in response to a determination that said reservation request can be validated based on user information within said source workstation, means for determining whether or not the capacity of said network is sufficient to meet requirements of said reservation request (*see,* page 4, lines 19-22, describing a second verification performed, in addition to the user verification, to determine whether network capacity is sufficient to meet the reservation request requirements; page 9, line 32 through page 10, line 7, explaining with reference to **FIG. 3**, that the if the user verification performed at step **52** fails, the reservation request is rejected and if the user verification is successful, the process continues with an assessment of network capacity (step **54**); and

in response to a determination that the capacity of said network being sufficient to meet requirements of said reservation request, means for establishing a virtual connection from said ingress node to said egress node (*see,* page 4, lines 22-26, describing virtual connection establishment performed in response to the network capacity verification; page 10, line 5 through page 11, line 2, describing with reference to **FIG. 3** that if at step **58** it is determined that network capacity is sufficient to accommodate the reservation request, virtual connection establishment continues with setting a flow identification (step **64**), updating a network database **56** (step **66**), and sending a reservation request acceptance (step **62**)).

GROUNDS OF REJECTION TO BE REVIEWED ON APPEAL

A. The rejection of claims 8-14 and 16-22 under 35 U.S.C. §103(a) as being unpatentable over U.S. Patent Number 6,694,429 issued to Kalmanek, Jr. et al. (hereinafter "*Kalmanek*") is to be reviewed on Appeal.

B. The rejection of claims 15 and 23 under 35 U.S.C. §103(a) as being unpatentable *Kalmanek* in view of U.S. Patent Number 6,768,738, issued to Yazaki et al. (hereinafter "*Yazaki*") is to be reviewed on Appeal.

ARGUMENT

A. Since *Kalmanek* does not disclose or render obvious each claimed feature of independent claims 8 and 16, the rejection of claims 8-14 and 16-22 under 35 U.S.C. §103(a) as being unpatentable over *Kalmanek* is not well founded and should be reversed.

Appellants' invention is directed to utilizing a novel reservation protocol to establish a virtual connection. The manner by which the invention establishes the virtual connection reservation enables Quality of Service (QoS) standards to be applied to an ordinarily connectionless transmission layer, such as the Internet Protocol (IP) layer. A key feature of the claimed invention is a two-part, sequentially significant verification relating to whether a virtual connection reservation request will be granted or denied. Namely, a reservation server first uses user information (user permissions, etc.) to validate the virtual connection reservation request. Next, and in response to user information validation of the request, the request is validated in terms of available network capacity.

Specifically, claim 8, representative also of claim 16, recites a method "for reserving a virtual connection from a source workstation to a destination workstation" comprising, in part, steps of "determining whether or not said reservation request can be validated based on user information within said source workstation, wherein said user information is accessible by said reservation server" and "in response to a determination that said reservation request can be validated based on user information within said source workstation, determining whether or not the capacity of said network is sufficient to meet requirements of said reservation request."

The particular sequence and dependence of these two steps (i.e. that the network capacity verification follows and is in fact triggered by an affirmative result in the user verification step) is particularly important as it relates to otherwise connectionless layers such as IP in which checking network capacity may be time consuming and processing intensive. As explained in the specification background at pages 2-3, unlike connection oriented networks such as Asynchronous Transfer Mode (ATM), packet-switched protocol network layers are largely controlled on a device-by-device level. Under such circumstances, assessing network capacity through several nodes may require substantial processing resources and time. Appellants' claimed two-part, sequentially dependent verification in which a positive user verification is required to commence the network capacity check therefore dramatically improves the efficiency of the claimed reservation of a virtual connection when applied to ordinarily connectionless networks. Appellants' specification provides direct support for the foregoing limitations at page 9, line 32 through page 10, line 7, explaining with reference to **FIG. 3**, that the if the user verification performed at step **52** fails, the reservation request is rejected and if the user verification is successful, the process continues with an assessment of network capacity (step **54**)

Appellants respectfully disagree with the assertion on pages 2-3 of the final Office Action that *Kalmanek* discloses a step of determining whether or not the capacity of said network is sufficient to meet requirements of said reservation request in response to a determination that said reservation request can be validated based on user information within said source workstation. At col. 10, line 47 through col. 11, line 2 *Kalmanek* explains only generally that processing capacity is a factor determining whether a given management system can handle per-call and multiple-call reservation and handling. While user authorization checks are discussed at col. 10, lines 19-32, *Kalmanek* fails to provide any disclosure or suggestion of advantageously combining a user and network capacity verifications in the sequentially dependent manner recited in Appellants' claims.

Since Kalmanek fails to teach or suggest a step of determining network capacity sufficiency in response to a positive user information validation, the rejection of claims 8, 16, and claims 9-14 and 17-22 depending therefrom should be reversed.

B. The rejection of claims 15 and 23 under 35 U.S.C. §103(a) as being unpatentable *Kalmanek* in view of *Yazaki* is not well-founded and should be reversed.

Claims 15 and 23 are directly or indirectly dependent on the independent claims 8 and 16 which, as contended above by Appellants, have been incorrectly rejected under the references. By extension, the rejections of claims 15 and 23 are not well founded and should be reversed.

CONCLUSION

Appellants have pointed out with specificity the error in the grounds for rejecting the claims, and the claim language that renders the invention patentable over the prior art references. Appellants therefore respectfully request that the claim rejections be reversed and this case be remanded.

Respectfully submitted,

Matthew W. Baca
Reg. No. 42,277
DILLON & YUDELL LLP
8911 N. Capital of Texas Highway
Suite 2110
Austin, Texas 78759
512-343-6116

ATTORNEY FOR APPELLANT

CLAIMS APPENDIX

1. (Cancelled)

2. (Cancelled)

3. (Cancelled)

4. (Cancelled)

5. (Cancelled)

6. (Cancelled)

7. (Cancelled)

8. A method for reserving a virtual connection from a source workstation to a destination workstation within a network to allow data packets to be transmitted between an ingress node of said source workstation and an egress node of said destination workstation, said method comprising:

sending a reservation request for a virtual connection from said source workstation to a reservation server, wherein said reservation server includes connection setup means for setting up a virtual connection that meets a predefined Quality of Service (QoS) requirement from said ingress node to said egress node;

determining whether or not said reservation request can be validated based on user information within said source workstation, wherein said user information is accessible by said reservation server;

in response to a determination that said reservation request can be validated based on user information within said source workstation, determining whether or not the capacity of said network is sufficient to meet requirements of said reservation request; and

in response to a determination that the capacity of said network being sufficient to meet requirements of said reservation request, establishing a virtual connection from said ingress node to said egress node.

9. The method of claim 8, wherein said determining whether or not said request can be validated further includes:

verifying an authentication of a user associated with said user information; and

verifying user rights of said user to obtain said virtual connection.

10. The method of claim 8, wherein said method further includes in response to an insufficient capacity of said network with respect to a previous reservation request, delivering a new reservation request from said source workstation to said reservation server, wherein said new reservation request includes new parameters that are set in accordance with the capacity of said network as reported from said reservation server to said source workstation.

11. The method of claim 8, wherein said method further includes delivering from said reservation server to said ingress and egress nodes information required to set up a virtual connection from said ingress node to said egress node and a flow identification of communications to be established such that said ingress node may transmit any data packet received from said source workstation over said virtual connection.

12. The method of claim 11, wherein said information sent by said reservation server to said ingress and egress nodes to set up a virtual connection includes a FlowID identifying a flow that corresponds to communications to be established over said virtual connection.

13. The method of claim 12, wherein said method further includes comparing a FlowID of a new packet received by said ingress node with at least one FlowID corresponding to at least one reserved virtual connection that has been established from said reservation server to said ingress node.

14. The method of claim 12, wherein said method further includes delivering a RouteID from said reservation server to said ingress and egress nodes, wherein said RouteID identifies a route already known by said ingress and egress nodes.

15. The method of claim 11, wherein headers of all packets belonging to a flow using said virtual connection includes a source address, a destination address, a port number, and a Quality of Service identifier.

16. An apparatus for reserving a virtual connection from a source workstation to a destination workstation within a network to allow data packets to be transmitted between an ingress node of said source workstation and an egress node of said destination workstation, said apparatus comprising:

means for sending a reservation request for a virtual connection from said source workstation to a reservation server, wherein said reservation server includes connection setup means for setting up a virtual connection that meets a predefined Quality of Service (QoS) requirement from said ingress node to said egress node;

means for determining whether or not said reservation request can be validated based on user information within said source workstation, wherein said user information is accessible by said reservation server;

in response to a determination that said reservation request can be validated based on user information within said source workstation, means for determining whether or not the capacity of said network is sufficient to meet requirements of said reservation request; and

in response to a determination that the capacity of said network being sufficient to meet requirements of said reservation request, means for establishing a virtual connection from said ingress node to said egress node.

17. The apparatus of claim 16, wherein said determining whether or not said request can be validated further includes:

means for verifying an authentication of a user associated with said user information; and

means for verifying user rights of said user to obtain said virtual connection.

18. The apparatus of claim 16, wherein said apparatus further includes in response to an insufficient capacity of said network with respect to a previous reservation request, means for delivering a new reservation request from said source workstation to said reservation server, wherein said new reservation request includes new parameters that are set in accordance with the capacity of said network as reported from said reservation server to said source workstation.

19. The apparatus of claim 16, wherein said apparatus further includes means for delivering from said reservation server to said ingress and egress nodes information required to set up a virtual connection from said ingress node to said egress node and a flow identification of communications to be established such that said ingress node may transmit any data packet received from said source workstation over said virtual connection.

20. The apparatus of claim 19, wherein said information sent by said reservation server to said ingress and egress nodes to set up a virtual connection includes a FlowID identifying a flow that corresponds to communications to be established over said virtual connection.

21. The apparatus of claim 20, wherein said apparatus further includes means for comparing a FlowID of a new packet received by said ingress node with at least one FlowID corresponding to at least one reserved virtual connection that has been established from said reservation server to said ingress node.

22. The apparatus of claim 20, wherein said apparatus further includes means for delivering a RouteID from said reservation server to said ingress and egress nodes, wherein said RouteID identifies a route already known by said ingress and egress nodes.

23. The apparatus of claim 20, wherein headers of all packets belonging to a flow using said virtual connection includes a source address, a destination address, a port number, and a Quality of Service identifier.

EVIDENCE APPENDIX

Other than the Office Action(s) and reply(ies) already of record, no additional evidence has been entered by Appellants or the Examiner in the above-identified application which is relevant to this appeal.

RELATED PROCEEDINGS APPENDIX

There are no related proceedings as described by 37 C.F.R. §41.37(c)(1)(x) known to Appellants, Appellants' legal representative, or assignee.